PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Currently Amended) A method for secure transmissions, the method comprising:
determining a registration key specific to a participant in a transmission;
determining a first key;
encrypting the first key with the registration key;
sending the encrypted first key to the participant in the transmission;
determining a second key for decrypting content on a broadcast channel;
encrypting the second key with the first key;
updating the first key after a first time period has elapsed; and
updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key.

2. (Original) The method as in claim 1, wherein updating further comprises:
updating the first key according to a first time period; and
updating the second key according to a second time period, wherein the second time period is less than the first time period.

3. (Original) The method as in claim 2, wherein updating further comprises:
encrypting an updated first key with the registration key; and
encrypting an updated second key with the updated first key.

4. (Original) The method as in claim 2, further comprising:
encrypting a broadcast stream of information using the second key; and
transmitting the encrypted broadcast stream of information.

5. (Original) The method as in claim 4, wherein the broadcast stream of information comprises video information.

6. (Original) The method as in claim 4, wherein the broadcast stream of information comprises Internet Protocol packets.

7. (Original) The method as in claim 3, further comprising:

calculating a registration key information message; and

transmitting the registration key information message.

8. (Original) The method as in claim 7, further comprising:

calculating a first key information message corresponding to the updated and encrypted first key; and

transmitting the first key information message.

9. (Original) The method as in claim 8, further comprising:

calculating a second key information message corresponding to the updated and encrypted second key; and

transmitting the second key information message.

10. (Original) The method as in claim 1, further comprising:

transmitting the encrypted first key; and

transmitting the encrypted second key.

11. (Currently Amended) A method for secure reception of a transmission, the method comprising:

receiving a registration key specific to a participant in a transmission;

receiving a first key encrypted with the registration key;

decrypting the first key with the registration key;

receiving a second key for decrypting content on a broadcast channel;

decrypting the second key with the first key;

receiving a broadcast stream of information;

decrypting the broadcast stream of information using the second key;

receiving an updated first key after a first time period has elapsed; and

receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key.

12. (Original) The method as in claim 11, further comprising:

storing the first key in a secure memory storage unit; and

storing the second key in a memory storage unit.

13. (Original) The method as in claim 11, further comprising:

recovering the first key from a first key information message; and

recovering the second key from a second key information message.

14. (Original) The method as in claim 11, further comprising:

updating the first key according to a first time period; and

updating the second key according to a second time period.

15. (Currently Amended) In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:

a receive circuitry adapted to receive a registration key specific to a participant in a transmission, receive a first key encrypted with the registration key, ~~receiving~~ receive a second key for decrypting content on a broadcast channel encrypted with the first key, ~~receiving~~ receive an updated first key after a first time period has elapsed, and ~~receiving~~ receive an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key;

a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:

processing unit operative to decrypt key information;

memory storage unit for storing a registration key; and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message.

16. (Original) The infrastructure element as in claim 15, wherein the short-time key is processed by the user identification unit and passed to the mobile equipment unit.

17. (Original) The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

18. (Original) The infrastructure element as in claim 15, wherein the memory storage unit stores a broadcast access key, and wherein the processing unit decrypts the short-time key using the broadcast access key.

19. (Original) The infrastructure element as in claim 18, wherein the short-time key is updated at a first frequency.

20. (Original) The infrastructure element as in claim 19, wherein the broadcast access key is updated at a second frequency less than the first frequency.

21. (Original) The infrastructure element as in claim 15, wherein the broadcast service option is a video service.

22. (Currently Amended) A wireless communication system, comprising:

means for determining a registration key specific to a participant in a transmission;

means for determining a first key;

means for encrypting the first key with the registration key;

means for sending the encrypted first key to the participant in the transmission;

means for determining a second key for decrypting content on a broadcast channel;

means for encrypting the second key with the first key;

means for updating the first key after a first time period has elapsed; and

means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key.

23. (Currently Amended) An infrastructure element, comprising:

means for receiving a registration key specific to a participant in a transmission;

means for receiving a first key encrypted with the registration key;

means for decrypting the first key with the registration key;

means for receiving a second key for decrypting content on a broadcast channel;

means for decrypting the second key with the first key;

means for receiving a broadcast stream of information;

means for decrypting the broadcast stream of information using the second key;

means for updating the first key after a first time period has elapsed; and

means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel, and wherein the first part and the second part are concatenated to generate the second key.

24. (Currently Amended) A digital storage device, comprising:

first set of instructions for receiving a registration key specific to a participant in a transmission;

second set of instructions for receiving a first key encrypted with the registration key;

third set of instructions for decrypting the first key with the registration key;

fourth set of instructions for receiving a second key for decrypting content on a broadcast channel;

fifth set of instructions for decrypting the second key with the first key;

sixth set of instructions for receiving the broadcast stream of information;

seventh set of instructions for decrypting the broadcast stream of information using the second key; and

eighth set of instructions for updating the first key after a first time period has elapsed, updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel, and wherein the first part and the second part are concatenated to generate the second key.

25. (New) The digital storage device as in claim 24, wherein the first part includes a time value.

26. (New) The digital storage device as in claim 24, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.

27. (New) The method as in claim 1, wherein the first part includes a time value.

28. (New) The method as in claim 1, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.

29. (New) The method as in claim 11, wherein the first part includes a time value.

30. (New) The method as in claim 11, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.

31. (New) The infrastructure element as in claim 15, wherein the first part includes a time value.

32. (New) The infrastructure element as in claim 15, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.

33. (New) The wireless communication system as in claim 22, wherein the first part includes a time value.

34. (New) The wireless communication system as in claim 22, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.

35. (New) The infrastructure element as in claim 23, wherein the first part includes a time value.

36. (New) The infrastructure element as in claim 23, wherein the second key is generated by applying a cryptographic hash function to the concatenation of the first and second parts.